SECRET

6 September 1963

MEMORANDUM FOR: Director of Central Intelligence

SUBJECT : Security Aspects Resulting from the Dunlap Case

1. This memorandum submits recommendations for your approval; these recommendations are contained in paragraph 10.

2. In accordance with the request of the DCI, a review of the authority and responsibility of the DCI for the protection of sources and methods was conducted to define the extent of the DCI's authority within the community in view of the security problems in the Dunlap case. It was further requested that in consonance with such authority, appropriate action and recommendations be proposed for the improvement of community security systems.

3. Responsibilities of the DCI for the Protection of Intelligence

a. The statutory responsibility of the DCI is stated in Section 102 (d) of the National Security Act. Basically, the statute provides that it shall be the duty of the Agency, under the direction of the National Security Council --

"(1) to advise the National Security Council in matters concerning such intelligence activities of the Government departments and agencies as relate to the national security;

(2) to make recommendations to the National Security Council for the coordination of such intelligence activities of the departments and agencies of the Government as relate to the national security;

SECRET

(3) to correlate and evaluate intelligence relating to the national security, and provide for the appropriate dissemination of such intelligence within the Government using where appropriate existing agencies and facilities: Provided, That the Agency shall have no ... internal-security functions: ... And provided further, That the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure; ..."

Under the above statute, therefore, the DCI has a responsibility to advise on and to recommend to the National Security Council any measures the DCI deems appropriate for the implementation of his responsibility for protecting intelligence from unauthorized disclosure.

b. NSCID No. 1 provides in paragraph 2.a.(5) that CIA shall:

"Develop and review security standards and practices as they relate to the protection of intelligence and of intelligence sources and methods from unauthorized disclosure."

NSCID No. 1 further provides in paragraph 5:

"The Director of Central Intelligence, with the assistance and support of the members of the U. S. Intelligence Board, shall ensure the development of policies and procedures for the protection of intelligence and of intelligence sources and methods from unauthorized disclosure. Each department and agency, however, shall remain responsible for the protection of intelligence and of intelligence sources and methods within its own organization. Each shall also establish appropriate internal policies and procedures to prevent the unauthorized disclosure from within that agency of intelligence information

or activity. The Director of Central Intelligence shall call upon the departments and agencies, as appropriate, to investigate within their department or agency any unauthorized disclosure of intelligence or of intelligence sources or methods ...."

As set forth above, NSCID No. 1 provides that the USIB shall develop and review security standards and practices for the protection of intelligence sources and methods. The DCI, with the assistance and support of USIB, is to ensure the development of such standards and practices. It is to be noted, however, under the National Security Act of 1947, responsibility of the DCI for the protection of intelligence is a singular responsibility and there are no limitations defining how this responsibility is to be effected.

4. Limitations on DCI's Authority

The National Security Act of 1947, Section 102 (d), does not grant the DCI any specific authority with respect to protection of intelligence sources and methods in other departments and agencies. Security is traditionally considered a command function, and the responsibility of the head of each department and agency. Existing Executive Orders, NSCID's, and DCID's which enunciate security policy recognize this fact and place the implementation responsibility upon the head of each agency.

In summary, the National Security Act of 1947 places a responsibility on the Director of Central Intelligence, but does not grant any specific authority to implement that responsibility. Security policy within the community for the protection of intelligence has not been unilaterally formulated by the Director of Central Intelligence, but has been developed with the assistance and support of the USIB. Consequently, such policy has been affected by the departmental consideration of each USIB member agency which participates in the formulation of such policy.

5. Discussion

a. Briefly, the Dunlap case highlights certain factors in the intelligence community which are regarded as security weaknesses but which can be corrected. The following comments apply principally to

the State Department, Defense Department and the military services. The CIA, FBI and AEC each have special personnel security systems with the latter two having limited participation in intelligence activities.

(1) The assignment of military personnel to the most sensitive intelligence duties upon the basis of a limited and routine security investigation and clearance which was designed for the standard military duty assignment.

(2) The absence of expressed authority from DOD to NSA Security to investigate and polygraph military personnel assigned to NSA which limits the security control of one-sixth of the personnel working for NSA. Further, NSA Security has not been given the authority to extend their polygraphing of civilians to include all civilians presently "on board" in NSA. Definite improvements have been made in NSA Security since the Martin and Mitchell affair but despite public and Congressional pressures, the DOD has not seen fit to go this far for NSA Security.

(3) The non-acceptance by the State Department, the Defense Department, Navy, and the Air Force of the use of the polygraph as an aid in personnel security processing. Army has been favorable to the polygraph but has not established a policy or program in this regard. The polygraph, based on CIA and NSA experience, is a formidable asset in the field of personnel security which provides the greatest assurance of the integrity of intelligence personnel.

(4) The need to recognize and establish that the sensitivity of the intelligence community and activities therein are above and apart from the normal departmental and military duties and activities. Under this concept, the assignment to staff positions in the intelligence community or engaging in intelligence activities should require a special security clearance, including a

full field investigation and a voluntary polygraph, based on high security criteria. Security clearances for normal departmental or military duties are not sufficient and every civilian and military person for the present and the future should undergo the special security processing.

6. The extension of the use of the polygraph throughout the intelligence community would require a hard policy decision by the other agencies against their historical reservations on the use of the polygraph for personnel security processing. In addition, even if a favorable decision was made on the polygraph, it would take some time to develop a polygraph capability to cover the present intelligence community and keep current on the new personnel entering the community field. This, however, could be done but would have to be based on a time phase program. Each department would have to define those assignments outside of the staff positions of the intelligence community which would be considered as falling within the definition of sensitive intelligence collection activities.

7. As an example of the military security clearance problem, there are approximately 2,300 military personnel assigned to NSA. NSA Security has only security certifications by their parent service as to their clearance status. NSA does not have copies of investigations nor is NSA permitted to polygraph the military assignees. Many of these military assignees remain with NSA for some years. NSA Security takes control only when the military retire and seek to civilianize and continue their NSA duties. NSA Security after applying its civilian investigative criteria and using the polygraph rejects approximately 17 to 25% of the military seeking civilianized status. It is important to note that these rejectees may have worked for NSA for some years under their military status. Theoretically, this ratio of rejections between 17 and 25% could be projected to possibly mean that a considerable number of the current military strength at NSA would be unsuitable security-wise to NSA in a civilian status.

8. The CIA has had a related experience in military assignments to the Agency. The Agency, however, conducts its own investigation and polygraphs all such assignees even though these assignees generally have a Secret or Top Secret clearance with the military. Of the 502 proposed military assignees in the past 24 months the Agency has rejected 153 or a

total of 19% for security reasons. Obviously, there is a variance of security standards for access to sensitive intelligence upon the basis of the CIA and NSA experience with military assignees. In this regard it should be noted that there are some 138 military personnel detailed to NPIC and under the present arrangement the Agency has only a certification statement of their security status. The Agency does not investigate nor do we polygraph such personnel. In 1961 we proposed to the military services that all military assignees to NPIC be given polygraph interviews by their parent services. The Navy and the Air Force declined to polygraph their representatives; however, the Army was in full accord with the proposal. No further resolution of this problem has been obtained.

9. Discussion of Courses of Action for the DCI:

In view of the policy and the sizable administrative problems involved in recommending a program of special security criteria for participation in intelligence activities including a polygraph examination, the fullest cooperation of the departments and agencies would be necessary to effectuate such a program. In reference to the authorities of the DCI set forth above, it is felt that the logical course of action would be through the mechanism of a study by the Security Committee with recommendations to the USIB. This action would be consonant with the DCI's statutory responsibilities and the responsibilities set forth in NSCID No. 1. The DCI could supplement this action through direct conversation with the Department heads. If, however, the USIB consideration is inconclusive and steps were not taken to adequately cover the above-mentioned problems, the DCI would still have under his authorities the opportunity of taking this matter to the National Security Council and the President under both his statutory authority and NSCID No. 1. It is felt that the first course of action would properly and logically be through the mechanism of the USIB.

10. Accordingly, the following courses of action are recommended to the DCI:

a. That as an immediate step the Secretary of Defense be encouraged to grant adequate authority to NSA Security to polygraph all military and civilian employees now on duty at NSA who have not been at this time accorded polygraph interviews and that as part of the regular processing of employment, all future military and civilian employees be accorded polygraph interviews.

b. That the DCI direct the Security Committee to submit recommendations to the USIB concerning the following security proposals.

(1) That all personnel occupying staff positions in the intelligence components of the USIB be required to meet special personnel security criteria based upon a full field investigation equating to that of a sensitive position as defined in Executive Order 10450.

(2) That all personnel outside of the staff positions of the intelligence components of the USIB agencies engaged in the collection of intelligence or in intelligence activities be accorded full field investigations equating to that of a sensitive position as defined in Executive Order 10450. The departments and agencies of the USIB shall define those activities and positions which fall within this definition.

(3) That as a matter of policy all persons so assigned to positions defined in b. (1) and (2) above be accorded a voluntary polygraph interview as an integral part of the security processing for approval to occupy these positions. Further, that a program be immediately initiated to develop polygraph capabilities to meet this requirement, further recognizing that the completion of this program will involve considerable time.

(4) That the assignment to intelligence duties require the meeting of special security criteria as a condition of assignment and that failure to meet such criteria or unwillingness on the part of the individual to submit to such criteria will cause the individual to be returned to his parent service for assignment or other disposition as deemed appropriate.

(5) Such other recommendations that the Security Committee may deem necessary and appropriate.

R. L. Bannerman
Director of Security

CONCUR:

Deputy Director
(Support)

Date

The recommendation in paragraph 10 is approved.

Date

John A. McCone
Director of Central Intelligence

Distribution:
Orig. - Return to OS
1 - ER
2 - DD/S
1 - Deputy General Counsel

SECRET

6 September 1963

MEMORANDUM FOR: Chairman, United States Intelligence Board

SUBJECT: Security Considerations Resulting from the Dunlap Case

1. The Dunlap case raises serious questions as to the policy, practices and procedures employed in the intelligence community for the protection of intelligence and intelligence sources and methods. The serious security aspects of the Dunlap case and the damage to the national security resulting therefrom calls for an immediate review of our security policies for the protection of intelligence. The implications point to definite weaknesses in our personnel security procedures. It would appear that far-reaching corrective measures may be warranted. Certainly, a new look should be taken at security practices and procedures and I would propose that the Security Committee undertake an immediate study and review of our current procedures and present recommendations to the USIB.

2. In the recent past, consideration has been given to various ideas as to how the personnel security system could be greatly strengthened. These ideas concern the requirement for more thorough investigations of intelligence personnel and the possible use of a voluntary polygraph procedure. The administrative burdens and organizational problems of sharply upgrading the intelligence system are formidable and would require a considerable amount of time, money and effort in any drastic upward revision. As regards the use of the polygraph as an aid in personnel security clearances, there has been for policy and other reasons great reluctance to engage in a program of this nature. It is felt, however, that the present personnel security practices are inadequate to establish the security integrity of the vast number of persons now engaged in sensitive intelligence activities. A new approach must be introduced if the intelligence community is to assure itself of the reliability of its personnel and its great volume of sensitive information. I would suggest that the Security Committee consider, among others, the following proposals and submit recommendations to the USIB.

SECRET

a. That there is a need to recognize and establish that the sensitivity of the intelligence community and activities therein are above and apart from the normal classified departmental and military duties and activities of the departments and agencies of the USIB. Under this concept the assignment to or employment in intelligence activities requires a special security clearance and conformance to high security standards.

(1) That all personnel occupying staff positions in the intelligence components of the USIB be required to meet special security criteria based upon a full field investigation equating to that of a sensitive position as defined in Executive Order 10450.

(2) That all personnel, outside of the staff positions of the intelligence components of the USIB agencies, engaged in the collection of intelligence or in intelligence activities be accorded a full field investigation equating to that of a sensitive position as defined in Executive Order 10450. The departments and agencies of USIB shall define those activities and positions which fall within this definition.

b. That as a matter of policy all persons so assigned to positions defined in (a) (1) and (2) above be accorded a voluntary polygraph interview as an integral part of the security processing for approval to occupy those positions. Further, that a program be immediately initiated to develop polygraph capabilities to meet this requirement, further recognizing that the completion of this program will involve considerable time.

c. The assignment to intelligence duties requires the meeting of special security criteria as a condition of assignment and failure to meet such criteria or unwillingness on the part of the individual to submit to such criteria will cause the individual to be returned to his parent service for assignment or other disposition as deemed appropriate.

d. Such other recommendations that the Security Committee may deem necessary and appropriate.

Robert L. Bannerman
Chairman, Security Committee
USIB